Hong Kong University of Science and Technology

COMP170: Discrete Mathematical Tools for Computer Science

Spring 2009

Midterm Exam 2

21 April 2009, 3:00–4:20pm, LT-E

Instructions

1. This is a closed-book exam consisting of 7 questions.
2. Please write your name, student number and email address on the cover page of the answer booklet.
3. Please sign the honor code statement on the second page of the answer booklet.
4. All answers *must* be put on the answer booklet. Only the answer booklet needs to be handed in at the end of the exam.
5. In the answer booklet each question starts on a new page. This is for clarity and is not meant to imply that your answer needs to fill up all the space provided.
6. Unless otherwise specified, you *must* always explain how you derived your answer. A number without an explanation will be considered an incorrect answer.
7. Please put your student ID card on the desk so the TA can check it.
8. All mobile phones must be turned off completely during the exam or else you will be disqualified.

You may use the following identities in the exam without having to provide a proof:

1. $$\sum_{i=1}^{n} i^2 = \frac{2n^3 + 3n^2 + n}{6}.$$

2. For any real number $r \neq 1$,
$$\sum_{i=0}^{n-1} r^i = \frac{1 - r^n}{1 - r}.$$

3. For any real number $r \neq 1$,
$$\sum_{i=1}^{n} ir^i = \frac{nr^{n+2} - (n+1)r^{n+1} + r}{(1-r)^2}.$$

Question 1: [16 points]

Suppose Alice wants to send a message M to Bob using RSA encryption so that only Bob can read it. The plaintext M, as a single positive integer, is encrypted to the corresponding ciphertext C which is then sent to Bob. An adversary, Eve, intercepts the ciphertext in the communication channel and finds that $C = 22$. From a public directory, Eve finds that the public key (e, n) of Alice is $(47, 391)$ and that of Bob is $(173, 481)$. Eve wants to seek your help to break the RSA encryption to recover the original plaintext M.

What is the value of M? Describe in detail all steps required to compute it. In case you need to find the multiplicative inverse of a number, there is no need to show details of the extended GCD algorithm. You just need to provide a number and show that it is the multiplicative inverse.

Question 2: [12 points]

Suppose Alice and Bob want to share a secret key but the communication channel between them is not secure enough for the shared key to be sent directly.

They first agree on two integers m and n that do not have to be kept secret. Alice then chooses a secret integer a and Bob chooses a secret integer b. Since the channel is not secure, these two secret numbers will not be sent.

Propose a scheme with which Alice and Bob can share a secret key by performing appropriate operations on the numbers above. Explain why your scheme is secure. What is the value of the shared secret key?

Question 3: [16 points]

For each of the following parts, is the statement **true** or **false**?
You need to prove your answer, or else you will receive no mark even if the answer (**true** or **false**) is correct.

(a) When dividing 7^{1980} by 47, the remainder is 1.

(b) The statements

$$(p \wedge q) \Rightarrow r$$
$$(p \Rightarrow q) \Rightarrow r$$

are logically equivalent.

(c) $\exists x \in Z^+ \, (\forall y \in Z \, (x + y \geq 4))$,
where Z^+ is the set of positive integers and Z is the set of all integers.

(d) $\forall x \in Z^+ \, (6 \mid (x^3 - x))$,
where Z^+ is the set of positive integers and $\mid$ denotes 'is a divisor of' or 'divides'.

(e) If p is a prime number, then $p! + 1$ is prime.

Question 4: [10 points]

(a) Using the following three predicates:

$$\text{Smart}(x) : x \text{ is smart}$$
$$\text{Student}(x) : x \text{ is a university student}$$
$$\text{Politician}(x) : x \text{ is a politician}$$

write quantified statements for the following:

(i) All university students are smart.

(ii) Some politicians are not smart.

(b) Do the two statements in part (a) imply the following?

Some politicians are not university students.

Prove your answer using the quantified statements.

Question 5: [14 points]

In class we showed an algorithm for solving the Towers of Hanoi puzzle with $n \geq 1$ disks by making $2^n - 1$ moves.

Prove that $2^n - 1$ is the smallest number of moves required to move the n disks from the leftmost peg to the rightmost one.

Question 6: [14 points]

Prove the following:

> Every positive integer n can be expressed as
>
> $$n = a_r 2^r + a_{r-1} 2^{r-1} + \cdots + a_2 2^2 + a_1 2 + a_0,$$
>
> for some $a_0, a_1, \ldots, a_r \in \{0, 1\}$ and some nonnegative integer r.

Question 7: [18 points]

Consider the simultaneous recurrence relations below for all nonnegative integers n:

$$S(n) = \begin{cases} 1 & n = 0 \\ 3S(n-1) + 4 & n > 0 \end{cases}$$

$$T(n) = \begin{cases} 1 & n = 0 \\ 2T(n-1) + 3S(n-1) & n > 0 \end{cases}$$

By iterating the recurrences, find general non-recursive formulae for $S(n)$ and $T(n)$ without involving the summation ($\sum$) sign. Show all steps in your derivation. However, there is no need to use an inductive proof to prove the correctness of the formulae after you have derived them.

Is $\Theta(S(n)) = \Theta(T(n))$? Explain your answer.

SCRAP PAPER

SCRAP PAPER

SCRAP PAPER